Exhibit 83

SW-SEC00337355

From: Brown, Timothy [/O=SOLARWINDS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=2C7BCDFD72B7408CB161AB787299E231-TIMOTHY BROWN]
Sent: 9/7/2017 2:37:43 PM
To: Wehrmann, August [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=fffb30885e0b47b79c5c4b3ecf6d1b25-Wehrmann, Aug]; Raphael, David [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=51f855a4debb4e36add5ac70a5a0b5fd-David Raphael]; Lissy, Greg [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=54182c7a7aa144ecb7e9ead5d2ff80a6-lissy, greg]; West, Stacy [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a1efe635a54443fb8ac3a2a3a7cedbfb-Stacy West]; Day, Chris [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=e8d2b726fdc545f1b62d58cfd10f8e05-Chris Day]; Cullen, Mike [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=dd466d6de0914390b62052d8b9143023-Cullen, Mike]; Sobel, Dave [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=2defed22b7b6499f88ede820c47be809-David Sobel]; Dada, Gerardo [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=dada, gerardo8d8]; Pagliuca, John [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=1d9822ff66a74f81865e5be220f7874f-John Pagliuca]
CC: Wyatt, Joshua [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=d23b9a7071bd4cb0adbccad4a3f9c67b-Joshua Wyatt]; Van Steenbergen, Rene [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=d5ca2f709cad44b8a5bd0c6596302f78-Rene Van Stee]
Subject: Agenda and Slides for today's Monthly security synch
Attachments: MSP monthly security meeting Sept.pptx

Agenda,
Current state of security and proposed move to a proactive security model. Starting the investigation towards new security business opportunities.

Tim

solarwinds
Tim Brown | VP Security Architecture
Office: 512.498.6549 | Mobile: 518.879.6169


solarwinds
SEPTEMBER MSP SECURITY SYNC

AGENDA

solarwinds

- Moving towards a proactive security model
- MSP Security business Opportunities

CURRENT STATE OF SECURITY OPERATIONS

solarwinds

Technology	Core IT	MSP	Cloud
Network Security Palo Alto			
Vulnerability Scanning Managed Rapid 7			Unknown
Anti –Virus Managed SEP		25% SEP 75%Bit Defender	75% Bit Defender
Endpoint Encryption Bitlocker		Unknown	Unknown
Endpoint DLP Netskope			
Identity Management Okta, Thycotic SS, AD, Linux	AD accounts managed. Many gaps, inconsistent management.	AD accounts managed. But many gaps.	AD accounts managed. But many gaps
Security Log Management (SIEM)	AD Account management, Sensitive Group audit, VPN Activity,	AD Account management, Sensitive Group audit,	AD Account management, Sensitive Group audit, VPN Activity
Incident Response	Good for external events.	Good for external events	Good for external events
Internal security backlog management and prioritization			
Security Training employee			
Data Classification			
PEN Testing			
Policies Security, Data Retention, DR			
Operations review Helpdesk, HR, Support	Inconsistent training, policies and security procedures	Inconsistent training, policies and security procedures	Inconsistent training, policies and security procedures

CURRENT STATE OF PRODUCT/SERVICE SECURITY

solarwinds

Technology	Core IT	MSP	Cloud
Developer Security Training			
External Incident Response			
Internal security prioritization measurement and tracking	Inconsistent and not Measured	Inconsistent and not Measured	Inconsistent and not Measured
Use of commercial Code Scanners	Inconsistent use of free tools		
Application PEN testing strategy			
Security questions and response	On-premise applications face less scrutiny and in many cases require YES/NO answers	MSP customers are appropriately demanding for detailed answers	Cloud customers are appropriately demanding for detailed answers

- Developer training is inconsistent
- Security incidents identified by customer running commercial code scanner cost SW190K renewal
- Externally reported Security Incidents continue to grow (28 this year) Disrupt schedule, Have significant management and response costs
- Lack of legally approved security questions/answers are costing us time and customers (Faster response, more detailed response, and better capabilities)

A proactive security model

solarwinds

Risk Mitigation Plan for IT Security Operations

Lock down our critical assets that could cause a major event

- External PEN test of our environment – Provide a baseline
- Lock down administrative access and improve identity management process and procedures
- Implement Web Application FW to protect our critical web properties

Improve Cyber Hygiene so we are not a target of opportunity

- Improve coverage for endpoint security, encryption, event management
- Improve system scanning coverage, monitoring and patching
- Implement DLP on the endpoints
- Implement security training for all employee's

Focus on security areas that provide the biggest impact

- Coordinate IT Security Ops activities across all organizations. Standardize policies, share best practices and coordinate the measurement of risk for the organization
- Create legal approved security questionnaire answers.
- Reduce the number of security incidents by implementing industry standard best practices.

Risk Mitigation Plan for Product Security/Dev Ops

Establish a global, cross-pillar Security Champions – Product team members with 30% of their time dedicated to security. Dotted line report to VP Security Architecture

- Internal Training and Outreach
- Coordinate internal product security testing and application vulnerability scanning
- Internal bug bounty program
- Product Management and Engineering management coordination
- Measurement of risk and effectiveness of program per product line

Invest in Commercial code scanning tool

Invest in developer security training

Overall Budget Request:

Accelerate cross company adoption of all security controls

Security Program Manager	$180 IT/Dev Ops
Security Architect	$180 IT/Dev Ops
Application Firewall	$40K per year
Internal/External PEN test	$100K
Company wide Security Training $30K	
Secure development training	$30K
Commercial application code scanner $70K	
Total	**$680K +** 30%

time of 4 Security Champions

Risk of Non-Investment

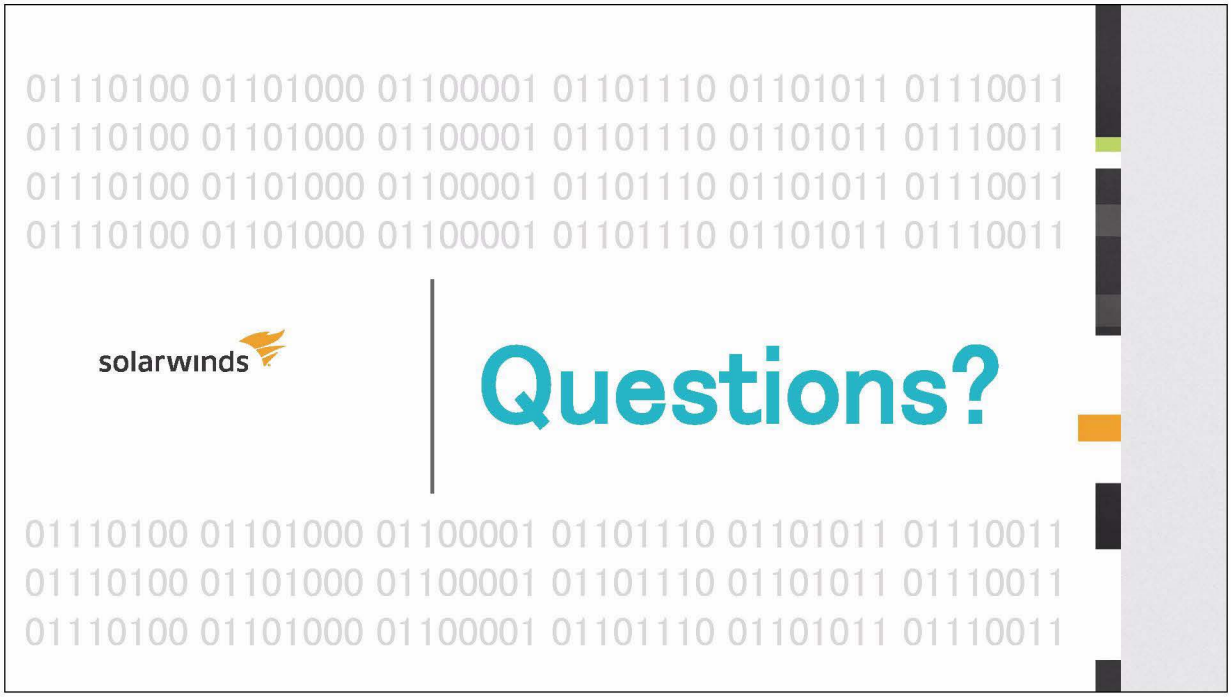
- Current state of security leaves us in a very vulnerable state for our critical assets. A compromise of these assets would damage our reputation and financially.
- Lack of cyber hygiene leaves us open to being a target of opportunity and a compromise will create downtime and lost revenue
- We have had 22 reported security incidents this year. Reactive responses costs significantly more than being proactive.
- We have lost a renewal of DPA for Accenture (192K) due to utilizing free code scanning tools that did not find all vulnerabilities.
- Without training our employees will continue to be one of our biggest risks
- Appropriate security policies, procedures, training, PEN testing are required by our commercial customers and asked for in qualifying questionnaires. Without appropriate answers we will lose business

5

MSP SECURITY BUSINESS OPPORTUNITIES

solarwinds

- Starting Investigation with Greg Lissy
- Areas of investigation
  - Multi-tier Endpoint protection (Good, Better, Best)
  - Network security – NGFW
  - IAM – Appropriate level of identity management
  - Security Training
  - GRC for smaller regulated environments (Healthcare, Finance, Education)


01110100 01101000 01100001 01101110 01101011 01110011
01110100 01101000 01100001 01101110 01101011 01110011
01110100 01101000 01100001 01101110 01101011 01110011
01110100 01101000 01100001 01101110 01101011 01110011
solarwinds
Questions?
01110100 01101000 01100001 01101110 01101011 01110011
01110100 01101000 01100001 01101110 01101011 01110011
01110100 01101000 01100001 01101110 01101011 01110011